Final Revision

2nd.Sec – Second Term "2023"

إعـــداد وتـــصميـــم/ جـــروب فـريـــق أصـــدقـــاء الكمبيوتـــر – أ/يـــاسمـيـن شـعـيـب

Final Revision Sheet

DEALING WITH THE WEBSITE DATA

➢ **Before creating search for term process we should shed the light on:**

- The looping concept.
- Some statement of looping in php language

We need in some programs to repeat a certain code many times or repeating it to a certain limit and this is what we will use when writing PHP code

➢ PHP language affords looping statement like

(For – While – do... While)

➢ Some examples on the usage of looping statements

➢ Using while statement:

```
1. <?PHP
2. $x = 1;
3. While ($x <=
   100)
4. {
5. Echo ($x);
6. Echo ("<Br>");
7. $x ++;
8. }
9. ?>
```

➢ Using For statement

```
1. <?PHP
2. For ($x = 1; $x <= 100; $x ++)
3. {
4. Echo ($x);
5. Echo ("<Br>");
6. }
7. ?>
```

➢ Using Do .....while statement

```
1. <?PHP
2. $x = 1;
3. DO
4. {
5. Echo ($x . "<Br>“)
6.  $x ++;
7. }
8. While ($x < = 100);
9. ?>
```

The looping statement	Explanation
While { }	It is used to execute unknown or un limited number of repetitions and these repetitions can be executed only on one condition at first, testing the condition and be sure the result is true. Example: searching in data base and searching the internet.
Do { } while	Is used in executing an unlimited or unknown number of repetitions , and you start in executing a repetitive circle once before testing the condition if it is true. Example { printing the primary value of the variable }
For { }	It is used to execute known or limited number of repetitions. It works the same way as while statement. Example (printing the email address of the ministry website 10 times).

THE MOST IMPORTANT CODES

Code	function
<Table> </Table>	Declaring Table
<Tr> </Tr>	(Declaring Row)
<Td> </Td>	(Declaring Columns)
<? Php	(The Start Of PHP Code)
?>	(End of PHP Code)
Include ("Header.Php") Include ("Connection.Php")	Including Header & Connection Pages With The current page.

$	(Declaring Variable Name)
("SET NAMES 'UTF8'")	To Deal With Arabic without strange symbol such as ????
(mysql_query)	result of the query in the variable
Select *	(searching for all the fields of the data table)
While	(looping statement)
echo	(print)
;	(end of php statement)

if(isset($_POST['submit']'))	Be sure of pressing on submit button
$ num	(number of records)
 	New line
<a >	(creating a hyperlink)

AN ENTRY IN SECURING WEBSITES

- **Securing websites is a necessity to stop penetration, which leads to many harms and negative results like:**

1. Stealing or losing important database that may lead to great problems in all fields.
2. Getting foundational or personal information and what harms it may cause
3. Showing unsuitable content that it might contains political, religious, ethical attitudes.
4. Deforming the image of the foundation or the person who owns the website generally.

THE PENETRATION CONCEPT

It's generally called **website hacking** by using the penetrator the hacker a way or **a weak program** that enables him to get the validity of controlling the website management or dealing with its database by any way (showing, deletion, editing and so on).

THE WAYS OF PROTECTING THE WEBSITE

1. **Protecting server** (website hosting)Protecting the website here is the responsibility of **the sever or website** hosting where it makes / sets **security options & controls.**
2. Protecting the website developers

- Be sure of the inputs before saving it in the database.
- Encrypt password.

- Managing the important website folders with strong passwords.
- Specifying the user's validity correctly and clearly.

SOME PRECAUTIONS TO KEEP SECURING THE WEBSITE

1- Keep software up to date

Be sure of the continual updating programs that are in use.

2- Dealing with error messages

It's necessary to know the possible errors & try to hide them. Because these errors make the website weak and easy to be penetrated.

3- The certainty of the correct input data validation from the user website visitor.

If this doesn't happen, it paves the way to penetrating the website. This through inserting inputs causes penetration, so one of the main bases of protecting from penetration is to be sure of the user input data.

For Example:

The certainty of the field contains values that don't exceed some or a number of letters or to be sure the field is not empty , that's by the (if) clause in the code of the used languages to be sure of the input data validity.

We can do that on two levels:

Firstly: using the server & by using php code

Secondly: the client server & by using java script code.

```
IF ($term !== "" && $trans !== "" && $defe !== ""
&&!empty($file)
{
The code that is executed for the certainty that the
previous variables are not empty.
}
```

Thirdly: Passwords:

Passwords should be complicated so it would be difficult to a penetrator to discover it, especially the server password and the site admin password and the database passwords.

Note:

For the private passwords of the websites users: we could force the user to insert passwords with special characteristics.

For example, a number of letters not less than 8 letters. There are capital letters with numbers and special signs.

passwords should be always kept encrypted by using one of the available encryption styles in php language like SHA function (salt password) or MD5 function

4-Avoid inserting SQL statement is usually known by SQL injection through dealing with sites:

A penetrator might try inserting special parameter inside SQL Statement, this through the site data base input form to be done on the data base without informing the designer & the in charge of site to give other results.

For securing that we use SQL real –escape– string sign to prevent inserting SQL statement to the data base.

5– Avoid writing XSS (Cross site scripting) code through the website.

The penetrator may insert a code in the web pages, So this may lead to negative effects and risks to both the user & the website owner.

For example:

If there is a form that allows the user to write a comment then show all comments successfully, the penetrator will use it to write java script code.

For example, when sending the comment to server, this code is stored in database, and when it is shown in HTML page the code is done this may redirect the user to another page and in it a harmful content or fishing page (it contains fake form to get important data from a user that visiting the site like passwords or a number of a visa card. We can avoid that by using suitable programming style like not allowing any script in the comments fields.

6– File Uploads:

- Allowing file uploads to your site may cause great risks.
- Be sure of the file identity, if the file was an image we should be sure of the file identity.

For Example

```
file = $_FILES['uploadedfile'];
$allowedExtensions = array("jpg","jpeg","gif","png");
if
(!in_array(end(explode('.',$file['name'])),$allowedExte
nsions))
{
echo ' : الملفات المسموح برفعها هي ...عفواًjpg, jpeg, gif, png';
exit(o);
}
```

The Certainty of file size which is needed to upload:

To be sure of the file size which is about to be uploaded on the server through the page, it should be about 1MB we write the following code:

```
IF ($file['size'] > 1024000) {echo ' {;' خطا: حجم الملف اكبر من ١
ميجابايت
```

Note

Function array

It creates new array which contains a group of elements

in_array (the element which meant to search in the array, array elements)

To be sure of the 1st parameter inside the elements of the array (2^{nd} parameter).

Function in_array

Function end

Is considered one of the arrays and meant to get back the value of the last element in an array.

Function explode

explode('.',$file['name'])

Its job is to transfer a variable to an array which contains several elements & gets two parameters:

1st: the ways of separation between the variable contents & it could be

(space- dash- pholo stop) in the example it is (.)

2nd: it is the variable content which is meant to turn it into a text, and it is ($filename).

7- Secure Socket Layer SSL :

It is a protocol to support secure dealing with web server and web browser through a mediator that's called certificate authority CA and could be translated by a translation sector, this affords secure pages which uses protocol HTTPS instead of the HTTP especially for the websites which deals with financial dealings or important data forms.

8. Using applications and security websites tools

After finishing designing the website, we should test the web security by using codes & similar ways to what penetrators use and sometimes it's called (pen testing or penetration testing.)

→ applications that testing website security against penetrations some of them are free or open source

one of the biggest open source applications that is used widely for testing web security.

Is good for SQL injection and testing XSS

OpenVas

Netsparker

CREATING REGISTRATION PAGE

(REG.PHP)

1. Design the page by using expression web program.

Note: -

Form is used for passing or sending all the data that exists in all the controls from the web to the web server.

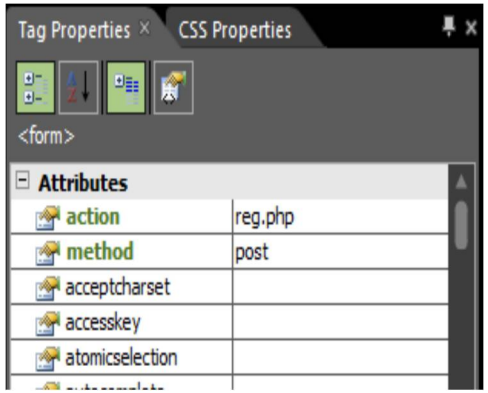
There are 2 ways for sending the form data:

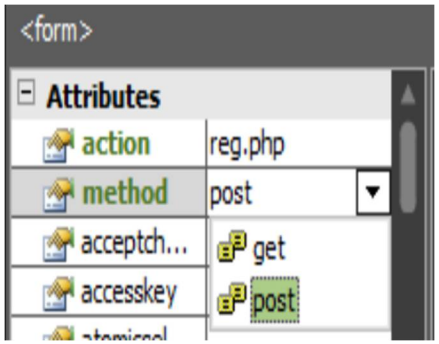
1- <form method="GET">

2- <form method="POST">

GET	POST
▪ the data is *little*. ▪ data is not secret because it *appears* on the *address line* of the internet screen. ◀	secret and secured data has been sent. (*important data*)

2. Adjust the form characteristics, be sure of specifying the value of post for the method as in the following figure.





الرقم	كود PHP
1	<?php session_start(); ?> Note we should write this code in the beginning of the page before the code
2	<?php include("header.php"); ?>

3	<?php
	include("connection.php");
	if(isset($_POST['Submit1']))
	{
	$txt_user=$_POST['txt_user'];
	$txt_pass=$_POST['txt_pass'];
	$txt_con=$_POST['txt_con'];
	mysql_query("SET NAMES 'utf8'");
	$query=mysql_query("insert into users values('','$txt_user','$txt_pass')");
	}
	?>

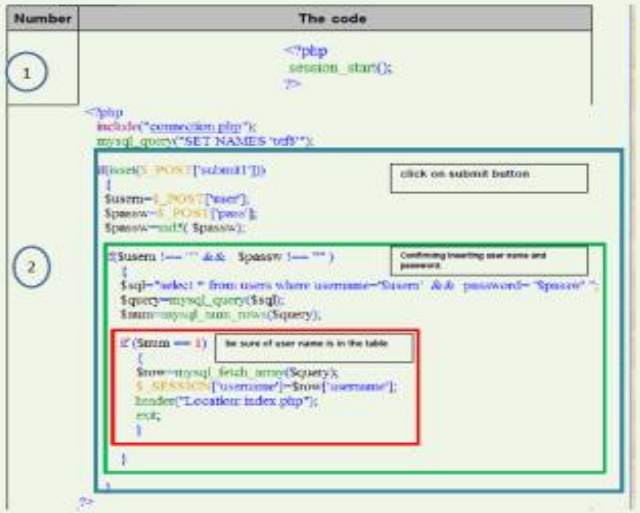
No.	PHP code	Explanation
1.	<?php session_start() ?>	It refers to the ad about using session inside the code of the page.
2.	<?php Include("header.php") ?>	The code refers to including header.php to registration page.
3.	<?php Include("connection.php") ?>	It refers to including the page that is connected to the database.
4.	If(isset($_post['submit']))	we use (if) statement to be sure of pressing on submit button
5.	$txt_user=$_POST['txt_user'];	User name (variable)
6.	$txt_pass=$_POST['txt_pass'];	Password (variable)
7.	$txt_con=$_POST['txt_con'];	Confirming password (variable)
8.	Mysql_query("SET NAMES'utf8'");	Solve the problem of dealing with data on the browser screen in Arabic language correctly without question marks.
9.	$query=mysql_query("insert into '$txt_user','$txt_pass')");users values(",	Used to add new data of a record to users table in the database.

After studying the possible procedures and its data in reg.php page and its effect on the inputs in user table. It is clear that the shape of the form, it has no security rules and Precautions, Because of the following reasons:

1. **There is no certainty of data validation like (accepting empty fields has no test for identical passwords.....).**

2. User name field in users table and this illogical, as there should not be more than one username with the same name.
3. The password is clear without encryption.

For treating these problems: we should do the following:

problem	solution
User name field in users table and this illogical, as there should not be more than one username with the same name.	*click on structure in MYSQL page then lick to make the field unique (Unique field doesn't accept repetition)*
Encryption of password.	*There are many methods for encrypting passwords one of them is using the query MD5.* *Function MD5 (message –digest algorithm)*
There is no certainty of data validation like (accepting empty fields has no test for identical passwords… …).	

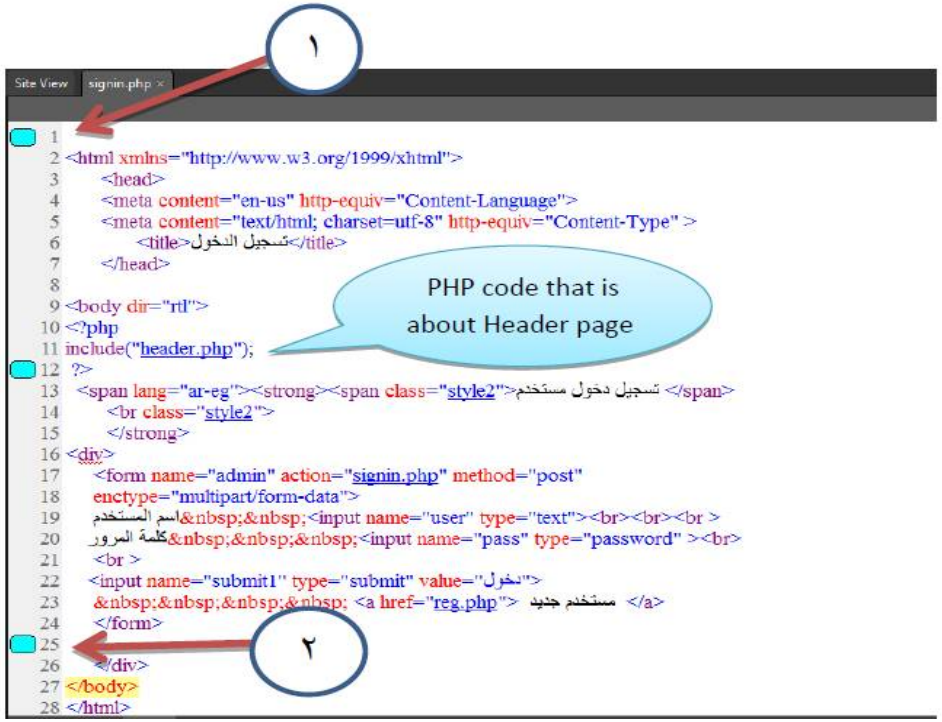
DESIGNING PAGE –SIGN IN PHP/

SIGN OUT .PHP

- Open expression web and design a page called sign in .php
- Insert form and insert on it controls
- Firstly: Creating signing in php by using expression web

2. Study the HTML code

3. Add the following php code instead of the following place in the previous code screen:




```
1
2 <html xmlns="http://www.w3.org/1999/xhtml">
3     <head>
4     <meta content="en-us" http-equiv="Content-Language">
5     <meta content="text/html; charset=utf-8" http-equiv="Content-Type" >
6         <title>تسجيل الدخول</title>
7     </head>
8
9 <body dir="rtl">
10 <?php
11 include("header.php");
12 ?>
13  <span lang="ar-eg"><strong><span class="style2">تسجيل دخول مستخدم </span>
14      <br class="style2">
15      </strong>
16 <div>
17     <form name="admin" action="signin.php" method="post"
18     enctype="multipart/form-data">
19     اسم المستخدم  <input name="user" type="text"><br><br><br >
20     كلمة المرور   <input name="pass" type="password" ><br>
21     <br >
22     <input name="submit1" type="submit" value="دخول">
23          <a href="reg.php"> مستخدم جديد </a>
24     </form>
25
26     </div>
27 </body>
28 </html>
```

PHP code	Explanation
$sql="select*from users where username='$usern' && password='$passw'";	Through select statement we search in users table in the database about the users name which is iserted and put in variables $Usern and and also search for the password that has been entered and put in variable on one condition the name & password are there together and identical with the inputs.
$num=mysql_num_rows($quary);	Mysql. Num –rows query is used to specify the number of registers which has been got and the number is stored in variable $ num.
If($num==1)	the last part of the signing in page variable$ num has been tested if its value equal 1 it means that there is only one user & his own password in users table. Note that: *if the value of variable $num equal (0) this means there is no record in users table by the input user and password , then the page stays as it is.*

Secondly designing signing out php page by using expression web

```
<?php
session_start();
 $_SESSION['username'] = "";
 header("Location: index.php");
 exit;
?>
```

THE WEBSITE SECURITY

PRECAUTIONS

After finishing designing all websites pages and so are signing in الجزيرة| out of a user. We should secure the site by the following: Adding the code of the beginning of the session we are asked to do it for the recorded user only as an entry .The aim is offering the ability to get the user's name as it is an entry only.

<?Php

session_start()

?>

```
<?php
 if(@$_SESSION['username'] == "")
     {
     echo ("  <a   href='signin.php'><span lang='ar-eg'>تسجيل الدخول</span> </a>");
     echo ("        ");
     echo "مستخدم غير مسجل";
     $_SESSION['username'] = "";
     }
else
     {
     echo ("  <a   href='signout.php'><span lang='ar-eg'>تسجيل الخروج</span></a>");
     echo ("        ");
     echo("مرحبا بكم". "   " . $_SESSION['username']);
     }
?>
```

Explaining the code

The conditional IF statement

if(@$_SESSION['username']=="")

- Php language deals with the sign @ as a variable.
- one of the php language rules is to put the sign $ before variable name.
- $ Session is variable in the server memory for the certainty that the user could sign in or not.

The condition that 's concerned with IF statement

it is tested if the user name equal null which means it's empty it has no data, there are two cases if it will be done or not.

o If the condition is true (yes)

Sign in becomes a hyperlink which is to sign in page that 's called sign in .php and leaves many spaces and print on the browser page the user isn't registered ,then variable session its value in the code is null:

.$_SESSION['username']="";

If the if condition isn't true.

It means: Session contains a value is the user name: then the sign out phrase becomes a hyperlink to sign out page that's called sign out.php, and leaves many spaces and print a welcome message on the browser page "you're welcome 'then leave many spaces, and write the user name that 's inserted in variable session by the code:

$_session [username]: you're welcome) Echo.